УПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНОЗДАТНОСТІ УКРАЇНИ: ПРАВОВІ ПРОБЛЕМИ І ПЕРСПЕКТИВИ ПОВОЄННОГО ПЕРІОДУ

Ніно Пацурія
доктор юридичних наук, професор, професор кафедри економічного права та економічного судочинства Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка
ORCID: 0000-0001-9974-3637

У статті розглядаються проблеми та перспективи впровадження новітніх інформаційно-комунікаційних технологій, зокрема штучного інтелекту (далі — ШІ), у сферу забезпечення національної безпеки та обороноздатності України. Досліджуються основні нормативно-правові акти, які містять положення про впровадження ШІ в оборонне та безпекове законодавство України; негативні та позитивні аспекти запровадження ШІ; європейський і світовий досвід застосування ШІ у вказаному напрямі. Порушено питання трансферу технологій ШІ через сферу безпеки та обороноздатності в інші галузі економіки.

Ключові слова: штучний інтелект, інформаційно-комунікаційні технології, національна безпека та обороноздатність України, оборонно-промисловий комплекс, трансфер технологій, правове регулювання штучного інтелекту, діджиталізація

Постановка проблеми. Усталена безпека — одне з наріжних питань, яке поставало перед Україною впродовж її багатовікової історії. Повномасштабна збройна агресія РФ проти України оголила численні загрози, що виникли не тільки перед нашою державою, а й перед всією світовою системою безпеки в цілому.

Забезпечення національної безпеки та обороноздатності України в повоєнний період має стати головним пріоритетом військово-політичного керівництва держави.

Досвід зарубіжних країн доводить, що швидке, ефективне та гнучке забезпечення потреб суспільства у воєнній безпеці та обороноздатності держави в повоєнний період досягається шляхом упровадження новітніх технологій, зокрема застосування ШІ та Big Data, як пріоритету подальшого розвитку оборонно-промислового комплексу повоєнної України. На сьогодні ШІ належить до таких технологічних сфер суспільного розвитку, які стрімко розвиваються та мають великий потенціал у багатьох галузях, включаючи національну безпеку, оборону, військову медицину, військову логістику, розвідку і контррозвідку, аеророзвідку тощо. Вказане пояснює суть обраної проблематики, актуальність і потребу в її дослідженні.

Літературний огляд. Дослідженню проблематики впровадження ШІ у сферу обороноздатності присвятили свої публікації такі вчені як В. Є. Хаустова, О. І. Решетняк, М. М. Хаустов, В. А. Зінченко [1], З. В. Гбур [14], М. О. Кизим, В. В. Шпілєвський,

О. В. Шпілєвський [12]. Проте у наведених дослідженнях недостатньо уваги приділено обґрунтуванню проблематики та перспектив упровадження ШІ у сферу забезпечення національної безпеки та обороноздатності України в повоєнний період; розгляду основних нормативно-правових актів, які містять положення про впровадження ШІ; негативним та позитивним рисам запровадження ШІ у вказаному напрямі; питанням трансферу технологій ШІ через сферу забезпечення національної безпеки та обороноздатності в інші галузі економіки.

Мета дослідження у статті: здійснити аналіз теоретичних і практичних аспектів застосування ШІ у сферу забезпечення національної безпеки та обороноздатності України у повоєнний період, виявити негативні та позитивні аспекти запровадження ШІ у сферу забезпечення національної безпеки та обороноздатності в цілому і запропонувати власні обґрунтовані висновки.

Виклад основного матеріалу. Оборонно-промисловий комплекс (далі — ОПК) стратегічно був, є і повинен стати джерелом запровадження новітніх технологій, у тому числі окремих інформаційно-комунікаційних технологій (далі — ІКТ). Виникнення, розвиток та стрімке поширення ІКТ, зокрема ШІ, надають поштовх інноваційним перетворенням ОПК і стають драйвером перетворень інших галузей економіки через інструмент трансферу технологій у різних країнах світу.

Підтвердженням важливості використання ШІ для забезпечення національної безпеки є результати досліджень Науково-технічної організації НАТО, що визначають найбільш суттєві з них для розвитку технологій, згідно з якими ключовими технологіями є ШІ, Big Data, автономні транспортні засоби, космос, гіперзвукові літальні апарати, квантові технології, біотехнології, нові матеріали тощо [1, 18].

Вказане повністю вкладається в концепт «Четверта промислова революція», який обґрунтовує, що драйверами розвитку світової економіки є інноваційні технології, які не лише кардинально змінюють усі галузі економіки, у тому числі ОПК, з метою забезпечення національної безпеки та обороноздатності, а й створюють абсолютно нові типи виробництва, які базуються на аналізі ШІ, Big Data, роботизації, доповненій реальності, Інтернеті речей (Internet thing) тощо. Фактично Індустрія 4.0 — це всі сфери життєдіяльності суспільства, на які можуть біти поширені новітні технології [2, 7].

З аналізу щорічних доповідей Стенфордського університету «Artificial Intelligence Index Report» відомо, що протягом останніх років багато держав розробили довгострокові національні Стратегії розвитку ШІ та здійснюють певні заходи щодо їх упровадження.

У цілому стратегії розвитку ШІ різних країн світу науковці поділяють на три основні групи: а) група, яка визначається реалістичним ставленням до формування стратегій ШІ, глибоким аналізом не тільки стану сфери застосування ШІ в країні, а й дійсних потреб її розвитку. Стратегії країн цієї групи мають фундаментальний характер і відображають як загальні світові проблеми впровадження ШІ, так і конкретні плани реінжинірингу різноманітних секторів ринку та бізнесу, цифровізації багатьох галузей національних економік та різних сфер суспільних відносин (Королівство Саудівська Аравія, США тощо); в) група країн, для яких характерним є ґрунтовний і прагматичний підхід до цілей та етапів їх досягнення з урахуванням дійсних потреб держави і формування окремих унікальних завдань та цілей розвитку ШІ (Велике Герцогство Люксембург, Республіка Мальта, Малайзія, Республіка Литва); с) група країн, стратегії яких виконані у формалізованому вигляді, налічують базові цілі розвитку країни в напрямі впровадження технологій зі ШІ в певних сферах суспільної життєдіяльності (Австралія, Республіка Австрія, Королівство Іспанія, Держава Катар, Португальська Республіка, Республіка Кіпр, Нова Зеландія, Держава Ізраїль, Швейцарська Конфедерація тощо) [3, 59–60].

Прагматичне питання, що виникає у зв'язку з викладеним вище: чи сформовано Україною стратегічне бачення використання можливостей ШІ у сфері забезпе-

чення національної безпеки та обороноздатності в контексті інтеграції в концепт «Індустрія 4.0»?

Наразі Україною прийнято шість програмних довгострокових документів у безпековому напрямі, які стосуються (прямо або опосередковано) питань національної безпеки та обороноздатності держави і торкаються проблематики використання ШІ, Big Data та сучасних ІКТ у вказаних сферах: 1) Стратегія забезпечення державної безпеки [4], якою передбачено, що основними завданнями державної політики у сфері забезпечення державної безпеки є завершення створення, подальший розвиток і посилення спроможності національної системи кібербезпеки, оптимізація координації її суб'єктів з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі; створення ефективної системи обміну інформацією між суб'єктами забезпечення державної безпеки та запровадження дієвих механізмів доступу суб'єктів забезпечення державної безпеки до державних електронних інформаційних ресурсів та автоматизованих інформаційних і довідкових систем, реєстрів, банків (баз) даних; 2) Стратегія національної безпеки України [5], згідно з якою: поточними та прогнозованими загрозами національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов є стрімкі технологічні зміни, насамперед в енергетиці та біотехнологіях, розробки у сфері ШІ, які докорінно трансформують економіку і суспільство в цілому; розробляються системи озброєнь на основі нових фізичних принципів із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері ШІ, створення нових матеріалів, робототехніки та автономних безпілотних апаратів; основне завдання розвитку системи кібербезпеки — гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації; Україна зміцнить бойовий потенціал Збройних Сил України, інших органів сил оборони шляхом: удосконалення та розвитку на основі сучасних технологій систем управління, телекомунікацій, розвідки, логістики; 3) Стратегія інформаційної безпеки [6], яка передбачає, що основними напрямами забезпечення інформаційної безпеки України є протидія дезінформації та інформаційним операціям, насамперед держави-агресора. Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань: створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі; 4) Стратегія кібербезпеки України [7], якою передбачено, що забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Розширення кола держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет, вказує на потребу в забезпеченні національної безпеки та обороноздатності України. Швидко змінюваний цифровий світ вимагає формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачаючи нові можливості для цифровізації всіх сфер суспільного життя; 5) Стратегія воєнної безпеки України [8], відповідно до якої на глобальному рівні основними аспектами воєнної безпеки є руйнування створеної після Другої світової війни системи міжнародної безпеки, підвищення рівня невизначеності та непередбачуваності безпекового середовища, яке характеризується, зокрема, конкуренцією держав у сфері космічних, квантових, інформаційних, кібернетичних, гіперзвукових, біологічних, нано- та інших технологій, розробленням на їх основі систем озброєнь з використанням нових фізичних принципів, робототехніки та новітніх мате-

ріалів, мілітаризацією навколоземного космічного простору. Визначені пріоритети можуть бути реалізовані шляхом виконання таких основних завдань: розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохопної оборони України; підвищення рівня боєздатності Збройних сил України та інших складових сил оборони з досягненням і підтриманням визначених спроможностей щодо вогневого ураження противника, застосування авіації та протиповітряної оборони України, контролю ближньої морської зони, ведення спеціальних операцій, територіальної оборони України, управління та всебічного забезпечення військ (сил), відбиття агресії в кіберпросторі (ведення кібероборони); 6) Стратегія розвитку оборонно-промислового комплексу України [9], згідно з якою створення умов для розвитку ОПК України здійснюється з використанням механізмів державно-приватного партнерства та військово-технічного співробітництва з іноземними державами для виробництва високоефективного озброєння, військової та спеціальної техніки для задоволення потреб Збройних сил України, інших органів сектору безпеки і оборони, збільшення експортного потенціалу оборонно-промислового комплексу України і є метою державної військово-промислової політики. Світовими тенденціями розвитку ОПК є, зокрема, високі темпи технологічних змін і перехід до нового технологічного укладу (штучний інтелект, розвиток нових технологій зв'язку, біотехнологій, електроніки тощо) ведуть до появи нових і скорочення старих ринків, серед виробників озброєнь загострюється конкуренція. Тенденціями розвитку озброєнь є те, що провідні держави світу здійснюють активні заходи з переозброєння своїх військ. Зміни способів ведення збройної боротьби формують нові потреби у розробленні озброєнь на основі нових фізичних принципів з використанням квантових, інформаційних, космічних, гіперзвукових технологій, біотехнологій, а також технологій у сфері штучного інтелекту, створюються нові матеріали, робототехніка та автономні безпілотні апарати, удосконалюються неядерні високоточні озброєння (далі — ВТО).

Окрім того, Кабінет Міністрів України розпорядженням від 12 травня 2021 року № 438-р затвердив План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки [10], згідно з яким на вказаний період передбачено низку заходів та законодавчих ініціатив, зокрема запровадження правового регулювання з питань формування державної політики у галузі ШІ; запровадження державної підтримки використання технологій ШІ в пріоритетних галузях економіки; упровадження технологій ШІ в національну систему кібербезпеки для проведення аналізу і класифікації загроз та вибору стратегії їх стримування і запобігання їх виникненню; визначення пріоритетних напрямів і основних завдань розвитку технологій ШІ в документах оборонного планування тощо.

Необхідно зазначити, що 23 лютого 2023 року Верховна Рада України ратифікувала Угоду між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027) [11], метою якої є зміцнення та просування потенціалу Європи в ключових сферах цифрових технологій. Документ створює передумови для участі України в програмі ЄС, яка надає додаткові стимули і можливості для цифрової трансформації пріоритетних галузей і сфер суспільного життя, розвитку цифрової економіки, ІТ-бізнесу, ШІ та підвищення рівня цифрових навичок громадян.

Отже, можемо констатувати, що європейський напрям цифровізації суспільства та розвитку і поширення ШІ підтриманий Україною на законодавчому рівні.

Наведене вище в цілому доводить, що в Україні сформовано бачення напряму розвитку спеціального законодавства застосування технологій ШІ на основі існуючих оборонних та безпекових потреб. Проте цілісний стратегічний документ, як-то *Стратегія розвитку ШІ у сфері забезпечення національної безпеки та обороноздатності України*, відсутній, обговорення не відбувається навіть на рівні проекту. Вказане можна визначити як правову лакуну, яка потребує негайного усунення.

Зазначене обумовлює підвищення наукового інтересу і наукових дискусій до впровадження технологій ШІ у сферу забезпечення національної безпеки та обороноздатності України в повоєнний період, напрямів їх застосування, впливу технологій ШІ на ОПК та забезпечення обороноздатності країн світу [1, 66–67] і трансферу технологій ШІ через оборонну та безпекову сфери в інші галузі економіки.

Науковці вказують, що розроблення правового регулювання застосування технологій ШІ наразі відбувається вкрай повільно стосовно стрімкого розвитку технологій ШІ, які одночасно охоплюють усі сфери суспільних відносин. Тому контроль за створенням та використанням ШІ необхідно здійснювати не тільки суто технічним регулюванням (вимоги, технічні стандарти, регламенти, оцінки відповідності технічним стандартам, контроль відповідності вимогам технічних регламентів, етичних стандартів), а й шляхом формування комплексного законодавства [3, 66–67].

Зрозуміло, що триваюча російська військова агресія змушує по-новому осмислити місію і завдання національного ОПК у повоєнний період. Відтворення тенденцій розвитку озброєнь стандартів НАТО в ОПК України має визначити концептуально нові засади розвитку оборонних технологій, зростання конкурентоспроможності озброєнь українського виробництва, посилить обороноздатність і національну безпеку, сприятиме економічному зростанню країни [12, 36].

Утім, поточна ситуація призвела до усвідомлення необхідності перегляду як існуючих (оперативних і тактичних) підходів до організації економіки воєнного часу, так і загальних (стратегічних) принципів подальшого повоєнного розвитку економіки України за умов наявності потенційної майбутньої загрози.

Прикладом успішного застосування такого стратегічного підходу є досвід Ізраїлю, де ОПК відіграє вагому роль у розвитку Армії оборони Ізраїлю (далі — АОІ) та інноваційної економіки країни в цілому. Сутність підходу полягає в тому, що бюджетні на інші видатки Ізраїлю, які спрямовуються у наукові дослідження, підготовку кадрів, військову медицину та інші напрями інноваційного розвитку АОІ, ОПК та сфери безпеки, переносяться в суспільне життя у вигляді будівельних, інформаційно-комунікаційних, промислових, медичних технологій тощо. Тобто активно застосовуються принципи конверсії та трансферу технологій [13, 96–97].

На підставі узагальнених даних, які збирались та акумулювались за допомогою сигнального, візуального, людського та інших видів інтелектів, наприклад, для АОІ було розроблено відповідні рекомендації. Завдяки цим рекомендаціям та програмам «Алхімік», «Євангеліє» і «Відділ мудрості» АОІ у травні 2021 року під час боїв у секторі Газа завдано інтенсивних точкових ударів по об'єктах ХАМАС і палестинського Ісламського джихаду, знищено значну кількість бойовиків. Успішне застосування ШІ в секторі Газа та наявні перспективи використання досвіду Ізраїлю в Україні дають підстави сподіватися на принципову зміну тактики ведення воєнних дій і забезпечення новітнім озброєнням українських військ у повоєнний період [14, 54–55].

У дослідженні «Штучний інтелект і національна безпека», здійсненому для конгресу США у 2019 році, стверджується, що головною причиною створення різних систем військового призначення, що володіють ШІ, є необхідність оперативного опрацювання структурованих і неструктурованих даних значних обсягів інформації (так званих великих даних), обумовлена постійним розширенням числа, номенклатури та технічних можливостей сучасних засобів добування інформації. За висновками фахівців, подібні системи найбільш корисні в розвідці, а також під час ідентифікації об'єктів у процесі обробки відео- та фотоматеріалів, отриманих із засобів видовий розвідки, наприклад, зображень літальних апаратів, кораблів, різних видів зброї, фізичних осіб тощо, зроблених під різними кутами, освітленням і в різному оточенні. Основним напрямом розвитку військових систем, які мають ШІ, є централізоване планування і координація проведення військових операцій різного масштабу в повітряному, кос-

мічному, кібер-, морському і наземному просторі. Традиційно технології ШІ широко застосовуються в автономних бойових і мобільних засобах, здатних діяти самостійно і продовжувати виконання завдання (або повертатися на задану позицію) в разі втрати зв'язку з центром управління. Відомими прикладами такої техніки є безпілотні літальні апарати (далі — БПЛА), автономні наземні машини, надводні та підводні апарати різного призначення тощо [14, 56].

Отже, світовий досвід запровадження ШІ у сферу національної безпеки та обороноздатності вказує на те, що на сьогодні жодний збройний конфлікт не може бути вирішений без використання новітніх видів озброєння та військових дій, заснованих на інформації, отриманої в ході ідентифікації об'єктів і цілей засобами сучасного обладнання розвідки [14, 54], і характеризується трансфером технологій ШІ через оборонну та безпекову сфери в інші галузі економіки.

Наведене вище вказує напрям формування перспективного національного законодавства в частині застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період та доводить ефективність застосування ШІ в ході збройних конфліктів різної локалізації.

Проте слід окремо наголосити, що, як і будь-яке явище реальної дійсності буття, тотальне застосування ШІ не позбавлене негативних рис. Вказана теза породжує питання: чи має прогресуюча перспектива застосування ШІ у сфері забезпечення національної безпеки та обороноздатності негативні наслідки?

Фахівці наголошують, що не треба ігнорувати можливі побічні ефекти застосування ШІ у сфері забезпечення національної безпеки та обороноздатності. Оскільки значення ШІ у цій галузі визначається саме високою швидкістю обробки великих масивів різнорідних даних, що дає змогу істотно скорочувати тривалість циклу управління військами і зброєю, то зворотною реакцією на такий процес може виявитися катастрофічне погіршення ситуації у разі прийняття рішень за неповними, неправильними, сфальсифікованими вихідними даними [14, 57].

Отже, світовий досвід застосування ШІ у сфері забезпечення національної безпеки та обороноздатності та безпосередньо у воєнних конфліктах потребує критичного підходу. Варто враховувати і визнані США обмеження щодо застосування ШІ у воєнних діях. Так, на початку 2020 року Міністерство оборони США, розуміючи можливі негативні наслідки дії «розумної» зброї, сформулювало *п'ять етичних принципів* використання систем ШІ у військових цілях:

1) відповідальність: військовий персонал повинен з належною увагою оцінювати дії ШІ, залишаючись повністю відповідальним за розроблення, розгортання і використання систем ШІ;

2) неупередженість: Міністерство оборони США має робити кроки для мінімізації небажаних відхилень у можливостях систем ШІ;

3) відстеження: військові системи ШІ та їх можливості повинні розроблятися і розвиватися таким чином, щоб персонал мав належний рівень розуміння технології, процесів розроблення та методів застосування. Для військового персоналу повинні бути доступні методології, дані й документація, що належать до використовуваних систем ШІ;

4) надійність: можливості військових систем ШІ повинні бути однозначними, чітко сформульованими. Безпека та ефективність таких можливостей повинні перевірятися випробуваннями та підтверджуватися протягом усього терміну служби;

5) підпорядкування: військові системи ШІ повинні повністю виконувати призначені для них завдання, проте військові повинні мати можливість виявляти та запобігати небажаним наслідкам використання ШІ. Військові також повинні мати можливість виводити з бою або вимикати системи ШІ, у яких були помічені відхилення в роботі [14, 59].

На переконання керівництва Об'єднаного центру штучного інтелекту США, американські військові не будуть оснащувати системами ШІ центри управління стратегічним озброєнням, адже за запуски балістичних ракет повинні завжди відповідати *тільки люди*, тобто рішення про застосування зброї масового ураження має бути прерогативою виключно людини [14, 60].

Однак застосування технологій ШІ у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період може допомогти в аналізуванні величезної кількості розвідданих з відкритим вихідним кодом, що виходить з нашої країни. Що ж до очікувань стосовно ШІ у військовому застосуванні протягом наступних десятиліть, то деякі його методи та технології визначать ключові передові військові технології. Так, важливість використання ШІ підкреслюється у звіті «Science & Technology Trends 2020–2040» Організації НАТО з науки та технологій під час формування стратегічних пріоритетів у сфері розвитку озброєння та прийняття політичних рішень для країн НАТО і для країн-партнерів. У звіті вказано, що до 2040 року очікується, що основними характеристиками, які будуть визначати більшість ключових передових військових технологій, будуть такі: інтелектуальність — використання інтегрованого ШІ, орієнтованого на знання аналітичних можливостей і симбіотичного ШІ людського інтелекту для забезпечення застосувань проривних технологій; взаємопов'язаність — експлуатація мережі віртуальних і фізичних доменів, включно з мережами датчиків, організацій, окремих осіб та автономних агентів, пов'язаних за допомогою нових методів шифрування та технологій розподіленого обліку; поширеність — використання децентралізованого та широкомасштабного зондування, зберігання й обчислення для досягнення нових руйнівних військових ефектів; цифровізація — цифрове поєднання людських, матеріальних та інформаційних областей для підтримки нових руйнівних ефектів [1, 19].

Таким чином, більшість напрямів технологічного розвитку військового потенціалу та обороноздатності пов'язані з розвитком ШІ. Цей вплив відбуватиметься переважно завдяки використанню вбудованого ШІ в інші супутні технології, такі як віртуальна/доповнена реальність; квантові обчислення; автономність, моделювання; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних.

Штучний інтелект матиме трансформаційний вплив на ядерні, аерокосмічні, кібернетичні технології, технології розробки нових матеріалів та біотехнології. Практики зазначають, що ці наслідки матимуть такий самий стратегічний вплив на зміну у військових технологіях, що й упровадження ядерної зброї [1, 22].

У якості проміжного висновку слід зазначити, що ШІ може бути використаний для створення систем розвідки та контролю, які можуть виявляти загрози національній безпеці та вживати заходів для їх запобігання. Він також може бути застосований для автоматизації та оптимізації військових операцій, що дає змогу зменшити ризики для життя військових та підвищити ефективність дій, у військовій логістиці, військовій медицині, аеророзвідці, у використанні БПЛА тощо.

Однак, разом з перевагами, ШІ може становити загрозу національній безпеці. Наприклад, країна-агресор може використовувати ШІ для здійснення кібератак та інших злочинів, що можуть негативно впливати на національну безпеку. Також існує ризик, що інші держави можуть використовувати ШІ для проведення кібершпигунства та кібератак на інфраструктуру країни.

У лютому 2023 року в Гаазі відбулася перша міжнародна конференція з відповідального використання ШІ у військовій сфері REAIM 23, скликана за ініціативою Нідерландів і Південної Кореї, за участю понад 60 країн. За підсумками саміту його учасники (за винятком Ізраїлю) підписали петицію про те, що країни, які вони представляють, висловлюють прихильність використанню ШІ відповідно до міжнародного права, не підриваючи принципів «міжнародної безпеки, стабільності та підконтрольності».

Серед питань, які також обговорили учасники REAIM 23, надійність військового ШІ, ненавмисні наслідки його використання, ризики ескалації та ступінь залученості людей до процесу ухвалення рішень. На думку критично налаштованих експертів, ця петиція, будучи необов'язковою до виконання, не розв'язує багатьох проблем, включно з використанням ШІ у воєнних конфліктах, а також БПЛА під управлінням ШІ тощо. І такі побоювання далеко не безпідставні. Так, один із найбільших військових підрядників США Lockheed Martin повідомив про те, що його новий навчальний винищувач, перебуваючи в повітрі приблизно 20 годин, увесь цей час керувався ШІ. А гендиректор Google Ерік Шмідт поділився своїми побоюваннями з приводу того, що ШІ може сам спровокувати воєнні конфлікти, зокрема із застосуванням ядерної зброї [15].

Висновки. Вказане дає нам змогу виокремити позитивні та негативні аспекти застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України у повоєнний період.

Позитивними аспектами варто вважати, зокрема:

- *підвищення ефективності:* ШІ може допомогти в зборі та аналізі великих обсягів даних, що забезпечує більш швидкий та точний аналіз інформації, скорочуючи час, необхідний для прийняття рішення;
- *мінімізація ризиків:* застосування ШІ може допомогти у попередженні катастроф та мінімізації ризиків для військового персоналу, що забезпечує безпеку та захист держави;
- *забезпечення безпеки:* ШІ може бути використаний для забезпечення безпеки країни, а саме, для забезпечення контролю над в'їздом та виїздом на кордоні, для виявлення та запобігання терористичним актам і злочинам;
- *автоматизація процесів:* ШІ може допомогти в автоматизації багатьох процесів у сфері оборони, що зменшує ризик помилок та підвищує ефективність;
- *удосконалення озброєння:* ШІ може бути використаний для розроблення та вдосконалення зброї, що забезпечує перевагу військам на полі бою.

Негативні аспекти використання ШІ у сфері забезпечення національної безпеки та обороноздатності України обумовлені таким:

- *етичні проблеми:* використання ШІ може порушувати етичні принципи та права людини, зокрема щодо конфіденційності особистих даних та використання зброї;
- *ризики безпеки:* використання автономної зброї, керованої ШІ, може створити ризики для безпеки і стати причиною аварій та непередбачуваних наслідків;
- *вразливість систем:* ШІ може стати мішенню для кібератак та вірусів, що може призвести до порушення діяльності та непередбачуваних наслідків;
- *залежність від технології:* застосування ШІ в забезпеченні обороноздатності може призвести до залежності від технології, що може стати проблемою в разі відмови техніки та відключення від мережі;
- *вартість:* використання ШІ в забезпеченні обороноздатності може мати дуже високу вартість та потребувати значних інвестицій у науково-дослідну роботу та розробку технологій.

Узагальнюючи, можна сказати, що для забезпечення національної безпеки та обороноздатності України у повоєнний період необхідно розробляти та впроваджувати у національне законодавство найкращі світові практики, що враховують потенційні можливості та загрози ШІ і забезпечують трансфер технологій ШІ через оборонну та безпекову сфери в інші галузі економіки. Необхідно забезпечити належний рівень кібербезпеки, захистити критичну інфраструктуру та розробити відповідні алгоритми та процедури для виявлення і запобігання загрозам.

Штучний інтелект може стати важливим інструментом у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період, допомагаючи збільшити ефективність та швидкість виконання військових завдань, знизити ризик втрат,

підвищити захищеність військових систем та зменшити витрати на оборону. Однак у ході розроблення та використання ШІ необхідно дотримуватися відповідних правових та етичних стандартів.

Перелік використаних джерел / List of references

1. *Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. БІЗНЕСІНФОРМ. 2022. № 3. С. 17–26.*
   Khaustova V. YE., Reshetnyak O. I., Khaustov M. M., Zinchenko V. A. Napryamky rozvytku tekhnolohiy shtuchnoho intelektu v zabezpechenni oboronozdatnosti krayiny. BIZNESINFORM. 2022. № 3. S. 17–26.
2. *Четверта промислова революція : зміна напрямів міжнародних інвестиційних потоків: монографія / А. І. Крисоватий, О. М. Сохацька, І. В. Скавронська [та ін.] ; за наук. ред. А. І. Крисоватого та О. М. Сохацької. Тернопіль: Осадца Ю. В., 2018. 480 с.*
   Chetverta promyslova revolyutsiya : zmina napryamiv mizhnarodnykh investytsiynykh potokiv: monohrafiya / A. I. Krysovatyy, O. M. Sokhats'ka, I. V. Skavrons'ka [ta in.] ; za nauk. red. A. I. Krysovatoho ta O. M. Sokhats'koyi. Ternopil': Osadtsa YU. V., 2018. 480 s.
3. *Костенко О. В. Аналіз національних стратегій розвитку штучного інтелекту. Інформація і право. 2022. № 2 (41). С. 58–69.*
   Kostenko O. V. Analiz natsional'nykh stratehiy rozvytku shtuchnoho intelektu. Informatsiya i pravo. 2022. № 2 (41). S. 58–69.
4. *Про Стратегію забезпечення державної безпеки: Указ Президента України від 16 лютого 2022 року № 56/2022.*
   Pro Stratehiyu zabezpechennya derzhavnoyi bezpeky: Ukaz Prezydenta Ukrayiny vid 16 lyutoho 2022 roku № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5 (дата звернення: 24.02.2023).
5. *Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020.*
   Stratehiya natsional'noyi bezpeky Ukrayiny: Ukaz Prezydenta Ukrayiny vid 14 veresnya 2020 roku № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 24.02.2023).
6. *Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021.*
   Pro Stratehiyu informatsiynoyi bezpeky: Ukaz Prezydenta Ukrayiny vid 28 hrudnya 2021 roku № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 24.02.2023).
7. *Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021.*
   Pro Stratehiyu kiberbezpeky Ukrayiny: Ukaz Prezydenta Ukrayiny vid 26 serpnya 2021 roku № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 24.02.2023).
8. *Про Стратегію воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021.*
   Pro Stratehiyu voyennoyi bezpeky Ukrayiny : Ukaz Prezydenta Ukrayiny vid 25 bereznya 2021 roku № 121/2021. URL: https://www.president.gov.ua/documents/1212021-3766 (дата звернення: 24.02.2023).
9. *Стратегія розвитку оборонно-промислового комплексу України: Указ Президента України від 20 серпня 2021 року № 372/2021.*

Stratehiya rozvytku oboronno-promyslovoho kompleksu Ukrayiny: Ukaz Prezydenta Ukrayiny vid 20 serpnya 2021 roku № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text (дата звернення: 24.02.2023).

10. *Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки: розпорядження Кабінету Міністрів України від 12 травня 2021 року № 438-р.*
Pro zatverdzhennya planu zakhodiv z realizatsiyi Kontseptsiyi rozvytku shtuchnoho intelektu v Ukrayini na 2021-2024 roky: Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 12 travnya 2021 r. № 438-r. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text (дата звернення: 24.02.2023).
11. *Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027): Закон України від 23 лютого 2023 року.*
Uhoda mizh Ukrayinoyu ta Yevropeys'kym Soyuzom pro uchast' Ukrayiny u prohrami Yevropeys'koho Soyuzu «Tsyfrova Yevropa» (2021–2027): Zakon Ukrayiny vid 23 lyutoho 2023 roku. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41298 (дата звернення: 24.02.2023).
12. *Кизим М. О., Хаустова В. Є., Шпілєвський В. В., Шпілєвський О. В. Військово-тактичні та економічні передумови розвитку оборонної промисловості України. Проблеми економіки. 2022. № 3 (53). С. 35–44.*
Kyzym M. O., Khaustova V. YE., Shpilyevs'kyy V. V., Shpilyevs'kyy O. V. Viys'kovo-taktychni ta ekonomichni peredumovy rozvytku oboronnoyi promyslovosti Ukrayiny. Problemy ekonomiky. 2022. № 3 (53). S. 35–44.
13. *Князєва О. А. Стратегічні вектори економічного розвитку країни у післявоєнний час. Науковий вісник Одеського національного економічного університету. 2022. № 3–4 (292–293). С. 94–100.*
Knyazyeva O. A. Stratehichni vektory ekonomichnoho rozvytku krayiny u pislyavoyennyy chas. Naukovyy visnyk Odes'koho natsional'noho ekonomichnoho universytetu. 2022. № 3–4 (292–293). S. 94–100.
14. *Гбур З. В. Можливість адаптації Ізраїльського досвіду використання штучного інтелекту у бойових діях на Сході. Інвестиції: практика та досвід. 2021. № 12. С. 54–61.*
Hbur Z. V. Mozhlyvist' adaptatsiyi Izrayil's'koho dosvidu vykorystannya shtuchnoho intelektu u boyovykh diyakh na Skhodi. Investytsiyi: praktyka ta dosvid. 2021. № 12. S. 54–61.
15. *Понад 60 країн погодилися з необхідністю контролю за зброєю зі штучним інтелектом.*
Ponad 60 krayin pohodylysya z neobkhidnistyu kontrolyu za zbroyeyu zi shtuchnym intelektom. URL: https://noworries.news/ponad-60-krayin-pogodylysya-z-neobhidnistyu-kontrolyu-za-zbroyeyu-zi-shtuchnym-intelektom/?fbclid=IwAR2r89Bt9-lKvGOFPAsue5wkACAFWNXpGEoxKbhWsZc5QlEJlE1jYJk7dnk (дата звернення: 24.02.2023).

Nino Patsuriia
Doctor of Legal Sciences/Dr. Habil. (Law), Professor, Professor of the Department of Economic Law and Economic Procedure of the Educational and Research Institute of Law of Taras Shevchenko National University of Kyiv

Implementation of Artificial Intelligence Technologies for Ensuring National Security and Defense Capability of Ukraine: Legal Issues and Prospects for the Post-War Period

The article discusses the problems and prospects of implementing modern information and communication technologies, including artificial intelligence, in the sphere of ensuring national security and defense capability of Ukraine. The main regulatory acts that contain provisions on the introduction of artificial intelligence in the defense and security legislation of Ukraine are investigated, as well as the negative and positive aspects of introducing artificial intelligence and the European and global experience of using artificial intelligence in this direction. The issue of transferring artificial intelligence technologies through the security and defense sector to other sectors of the economy is also raised. Ensuring national security and defense capability of Ukraine in the post-war period should become the main priority of the country's military and political leadership.

It is argued that the rapid, efficient, and flexible provision of society's needs for military security and defense of the state in the post-war period can be achieved through the introduction of advanced technologies, including the use of artificial intelligence and Big Data, as a priority for the further development of the defense industry complex of post-war Ukraine. Today, artificial intelligence belongs to such technological areas of social development that are rapidly evolving and have great potential in many fields, including national security, defense, military medicine, military logistics, intelligence and counterintelligence, aerial reconnaissance, and so on. This explains the essence of the chosen problematic, its relevance, and the need for its research.

It is concluded that the use of artificial intelligence in the sphere of ensuring national security and defense capability of Ukraine can have both positive and negative aspects. As a generalization, it is noted that in order to ensure national security and defense capability of Ukraine in the post-war period, it is necessary to develop and introduce the best world practices into national legislation, taking into account the potential opportunities and threats of artificial intelligence, and ensuring the transfer of artificial intelligence technologies through the defense and security sectors to other sectors of the economy.

Keywords: artificial intelligence, information and communication technologies, national security and defense capability of Ukraine, defense industry complex, technology transfer, legal regulation of artificial intelligence

Подано / Submitted: 24.03.2023
Доопрацьовано / Revised: 03.04.2023
Прийнято до публікації / Accepted: 11.04.2023